REMARKS

This Amendment is responsive to the Office Action dated October 15, 2004. All rejections and objections of the Examiner are respectfully traversed. Reconsideration is respectfully requested.

An interview was held on September 29, 2004 as to the fact that the change of address form previously submitted October 8, 2003 had not been entered, and accordingly the Office Action had not been received. Applicants wish to thank the Examiner for her kind consideration in restarting the period for response.

At paragraphs 1-6 of the Office Action, the Examiner rejected claim 18 for obviousness under 35 U.S.C. 103, citing a "Workshops" article in "Network Computing" by Gregory Yerxa ("Yerxa"), in combination with an article on online security in the publication "PC/Computing" by Ed Bott ("Bott"), as well as "Securing Java and ActiveX" by Anita Karve ("Karve"). Applicants respectfully traverse this rejection.

As discussed in the previous response, Yerxa discloses that the Java Virtual Machine (JVM) includes a Class Loader (CL), a Byte-Code Verifier (BCV), and a Security Manager (SM), that the SM is a Java class, and that the SM controls the performance of potentially dangerous activities. SM monitors file access, system I/O, network I/O, Class Loader instantiation, process/thread creation and access to Java class objects. Yerxa discloses that when an applet performs one of the actions monitored by the SM, the applet first consults the SM for approval. The SM decides if the action is permissible based on the origin of the application or applet. Whenever a potentially dangerous function is called from within the applet or application, the SM grants or denies access to specific resources based on the origin of the application or applet.

As also previously discussed, Yerxa specifically discloses that the Java system restricts ***access to*** applets and applications based on their origins. In this regard, Applets that are embedded in Web pages are most restricted, while local Java applications are trusted almost entirely without restrictions. Users may grant more access to certain applets, and this is enabled by denoting specific applets as trusted, thus overriding the normal default setting that all applets are untrusted and cannot access local information. Yerxa further teaches that an administrator can allow or deny specific access to the network based on an applet's origin. Bott discloses that Java and JavaScript are very dangerous, and advises users to disable them there machines to improve security. Bott also generally describes public key encryption, digital signatures, and digital certificates. Karve discusses aspects of Java and ActiveX relating to security, noting that Java applets may be signed using digital signatures associated with a developer and/or certificate authority (CA).

Nowhere in the combination of Yerxa, Bott and Karve is there disclosed or suggested any system for providing security against unauthorized access to internal resources of a network device including:

> means, within a security association manager, for receiving a digital signature ;
> means, within said security association manager, for accessing a de-encryption code associated with said digital signature, and for decrypting and authenticating said digital signature; and
> ***means, within a policy server, for receiving a request for allowed operations associated with said authenticated digital signature policy server; and***
> ***means, within said policy server, responsive to said request, and to a comparison of said authenticated digital signature with information within said policy server, for determining an access level for a java thread associated with said digital signature, and for sending an indication of said access level in a response to said security association manager.*** (emphasis added)

as in the present claim 18.

While Yerxa, Bott and Karve teach using digital signatures to control *access to* applets associated with the digital signatures, for purposes of determining the validity of the applets, with Karve specifically teaching the practice of ***authenticating the source of an applet*** based on the digital signature of the applet. Yerxa, Bott and Karve include no hint or suggestion of using a de-encrypted, authenticated digital signature to obtain an access level for a java thread, to be used while processing the java thread, as in the present claim 18. Thus the combined references fail to foresee even the desirability of using the contents of an authenticated digital signature to obtain access level information to be used to control access to system resources while processing a portion of program code, which is an advantage of the present system as set forth in claim 18.

For the above reasons, Applicants respectfully urge that the combination of Yerxa, Bott and Karve does not disclose all the features of the present independent claim 18. Accordingly, the combination of Yerxa, Bott and Karve does not form the basis for a *prima facie* case of obviousness under 35 U.S.C. 103 with regard to claim 18. Reconsideration of claim 18 is respectfully requested.

At paragraph 7 of the Office Action, the Examiner indicated that claims 6-7 and 12 were allowed.

For the above reasons, Applicants respectfully urge that the Examiner's rejection of claim 18 should be withdrawn.

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone the undersigned Attorney at 617-630-1131 so that such issues may be resolved as expeditiously as possible.

In view of the above amendments and remarks, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

JANUARY 10 2005
Date

D. J. C. T.

David A. Dagg, Reg. No. 37,809
Attorney/Agent for Applicant(s)
Steubing McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-300